

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-275114

(43)公開日 平成10年(1998)10月13日

(51)Int.Cl.<sup>9</sup>

G 0 6 F 12/14  
12/00  
15/00

識別記号

3 1 0  
5 3 7  
3 3 0

F I

G 0 6 F 12/14  
12/00  
15/00

3 1 0 K  
5 3 7 A  
3 3 0 D

審査請求 未請求 請求項の数2 O L (全 7 頁)

(21)出願番号 特願平9-80909

(22)出願日 平成9年(1997)3月31日

(71)出願人 000003273

富士通株式会社  
神奈川県川崎市中原区上小田中4丁目1番  
1号

(72)発明者 磯山 朋宏

岡山県岡山市磨屋町10番12号 株式会社富  
士通岡山システムエンジニアリング内

(72)発明者 荻江 裕司

岡山県岡山市磨屋町10番12号 株式会社富  
士通岡山システムエンジニアリング内

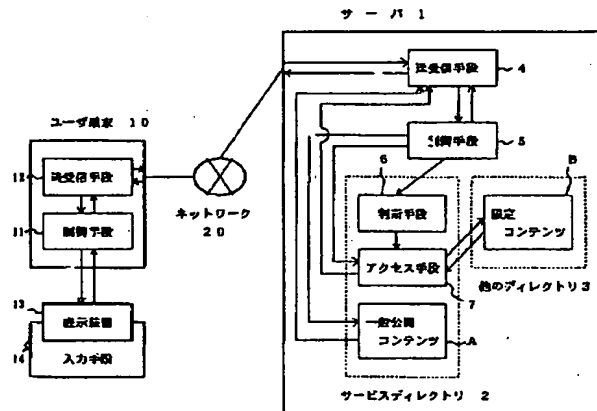
(74)代理人 弁理士 福井 豊明

(54)【発明の名称】 インターネットのコンテンツセキュリティ方法およびシステム

(57)【要約】

【課題】 インターネットのシステムにおいて利用されるインターネットのコンテンツセキュリティ方法およびシステムに関するものである。

【解決手段】 ユーザが自由に閲覧することができるサーバ上のサービスディレクトリ以外の他のディレクトリに特定用途の限定コンテンツを設け、ユーザ端末より特定のパラメータを与えることによって、上記限定コンテンツへのアクセス許可が与えられた場合に上記限定コンテンツにアクセスする。よって、上記限定コンテンツへのアクセス許可が与えられた者だけが該限定コンテンツへアクセスすることができ、アクセス許可が与えられていない者が該限定コンテンツへアクセスすることを確実に防止することのできる。



BEST AVAILABLE COPY

**【特許請求の範囲】**

【請求項1】 ユーザが自由に閲覧することができるサービスディレクトリをサーバ上に設け、ユーザ端末より特定のパラメータを与えることによって、上記サービスディレクトリに設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツへのアクセス許可が与えられるインターネットのコンテンツセキュリティ方法において、

上記限定コンテンツを上記サーバ上のサービスディレクトリ以外の他のディレクトリに設け、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に、上記限定コンテンツをアクセスすることを特徴とするインターネットのコンテンツセキュリティ方法。

【請求項2】 ユーザが自由に閲覧することができるサービスディレクトリをサーバ上に設け、ユーザ端末より特定のパラメータを与えることによって、上記サービスディレクトリに設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツへのアクセス許可が与えられるインターネットのコンテンツセキュリティシステムにおいて、

上記サーバ上のサービスディレクトリ以外の他のディレクトリに備えた上記限定コンテンツと、

上記サーバ上のサービスディレクトリに設けられるとともに、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツをアクセスするアクセス手段とを備えたことを特徴とするインターネットのコンテンツセキュリティシステム。

**【発明の詳細な説明】****【0001】**

【産業上の利用分野】 本発明はインターネットシステムにおいて利用されるインターネットのコンテンツセキュリティ方法およびシステムに関するものである。

**【0002】**

【従来技術】 現在、世界中にははるめぐらされたネットワークを介して接続された不特定多数のユーザがサーバ上に作成されたコンテンツを自由に閲覧することができるインターネットシステムが普及し、その中で特定のユーザだけを対象としたサービスも増加している。このサービスは、ユーザID、パスワード等を管理し、パスワードチェックでアクセスの許可が与えられた特定のユーザであると判断された場合に、特定のユーザを対象にして作成された限定コンテンツを閲覧することができるようにしている。以下、この従来のセキュリティシステムについて図4に基づいて説明する。

【0003】 インターネットシステムにおいて利用されるサーバ31上には閲覧ソフトであるブラウザによってユーザ端末33からネットワーク34を介して自由に閲覧することができるサービスディレクトリ32が設けられており、該サービスディレクトリ32に一般公開される一般公開コンテンツAおよび上記限定コンテンツB等

が編集されている。

【0004】 上記ユーザ端末33より一般公開コンテンツAのHTMLページを閲覧する場合、上記ブラウザより目的とするHTMLページのサーバアドレスおよびサーバ内アドレスであるURLを直接入力するか、または現在閲覧中のHTMLページ内に設けられたリンクを選択し実行することによってアクセスし閲覧することができる。

【0005】 また、上記ユーザ端末33より上記限定コンテンツBのHTMLページを閲覧する場合、上記一般公開コンテンツAの場合と同様にしてユーザIDおよびパスワード等の入力を行うHTMLページ（以下、パスワードページと言う）を表示させる。次に該パスワードページよりユーザIDおよびパスワードを入力すると、サーバ上に予め備えられたデータベースのデータに基づいて、上記のように入力されたユーザIDは存在するか、またパスワードが正しいか等のチェックが行われ、上記限定コンテンツBへのアクセス許可が与えられたユーザであると判断された場合に該限定コンテンツBにアクセスし閲覧することができる。

【0006】 しかしながら、一般にサーバ31上の上記サービスディレクトリ32に編集されたコンテンツは一般公開コンテンツA、限定コンテンツB等の区別に関係なく、上記ブラウザ上でこれらコンテンツのURLを直接入力することでアクセスすることができる。したがって、上記のような従来のセキュリティでは、上記パスワードページは一般公開コンテンツA等にリンクを設けるか、または直接URLを公開するなどしているのに対して、限定コンテンツBはそれ自体のURLを非公開とすることによって、上記パスワードページを経ないで上記限定コンテンツBにアクセスされることを防止している。

**【0007】**

【発明が解決しようとする課題】 上記のような従来のセキュリティでは、もし上記限定コンテンツBの場所すなわちURLが知られれば、アクセス許可が与えられていないユーザであっても、上記ブラウザ上で該URLを直接入力することで、上記限定コンテンツBへのアクセスを行うことができることになる。

【0008】 よって上記限定コンテンツBのURLは非公開とされているが、例えば一般公開および限定コンテンツBのURLが似かよっている場合に、アクセス許可が与えられていないユーザが一般公開コンテンツAのURLより上記限定コンテンツBのURLを類推して入力したり、また偶然に上記限定コンテンツBのURLを入力したりして上記限定コンテンツBのURLが知られてしまうことや、以前アクセス許可を有していたユーザが資格を喪失した後に、以前に知り得た上記限定コンテンツBのURLを利用することが起こりえる。

【0009】 以上のように従来のセキュリティでは、ア

クセス許可が与えられていないユーザによって上記限定コンテンツBへアクセスされることを完全に防止することができなかった。

【0010】本発明は上記の事情に鑑みて提案されたものであり、上記限定コンテンツへのアクセス許可が与えられたユーザだけが該限定コンテンツへアクセスすることができ、アクセス許可が与えられていないユーザが該限定コンテンツへアクセスすることを確実に防止することのできるインターネットのコンテンツセキュリティ方法およびシステムを提供することを目的とする。

【0011】

【課題を解決するための手段】本発明は上記目的を達成するために以下の手段を採用している。すなわち、ユーザが自由に閲覧することができるサービスディレクトリ2をサーバ1上に設け、ユーザ端末10より特定のパラメータを与えることによって、上記サービスディレクトリ2に設けたコンテンツのうち上記パラメータに対応した特定用途の限定コンテンツBへのアクセス許可が与えられるインターネットのコンテンツセキュリティ方法において、上記限定コンテンツBを上記サーバ1上のサービスディレクトリ2以外の他のディレクトリ3に設け、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に、上記限定コンテンツBをアクセスするという手段を採用している。

【0012】具体的には、上記サーバ1上のサービスディレクトリ2以外の他のディレクトリ3に備えた上記限定コンテンツBと、上記サーバ1上のサービスディレクトリ2に設けられるとともに、上記アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツBをアクセスするアクセス手段とを備えることによって実現する。

【0013】

【実施の形態】図1は本発明のインターネットのコンテンツセキュリティシステムの適用されるネットワークの概念図であり、図2は本発明のインターネットのコンテンツセキュリティシステムの一実施例のブロック図であり、図3は上記システムにおける処理手順を示すフロー図であり、以下図に基づいて説明する。

【0014】本実施例において、サーバ1上のサービスディレクトリ2にはパスワードページを含む一般公開コンテンツA、パラメータ判断手段6、アクセス手段7を、サービスディレクトリ2以外の他のディレクトリ3には限定コンテンツBを設けている。

【0015】ユーザ端末10よりネットワーク20を介して接続されたサーバ1上の上記限定コンテンツBを閲覧する場合、まず最初に上記サービスディレクトリ2に設けた上記パスワードページを表示させる。この手順は、上記ユーザ端末10のキーボードやマウス等の入力手段14で上記ユーザ端末の制御手段11により起動されたブラウザ上から直接上記パスワードページのURL

を入力するか、または一般公開コンテンツAのHTMLページ内に設けられた上記パスワードページのリンクを選択して実行(S1)すれば、上記パスワードページのURLがユーザ端末10の送受信手段12から、該URL中のサーバアドレスに基づいてネットワーク20を介して上記サーバ1の送受信手段4へ、次に該送受信手段4より制御手段5へ送られる(S2)。該制御手段5は送られたURL中のサーバ内アドレスに基づいて上記パスワードページを上記送受信手段4、ネットワーク20を介して上記ユーザ端末10の上記送受信手段12へ送る。次に上記ユーザ端末10では、送信されてきた上記パスワードページが上記ブラウザによって上記ユーザ端末10の表示装置13に表示される(S3)。

【0016】そして次に、該パスワードページにユーザが上記入力手段14によってパラメータとしてユーザIDおよびパスワードを与えて入力(S4)すれば、上記パスワードページのURLと同様に上記送受信手段12から上記ネットワーク20、上記サーバ1の送受信手段4を介して上記制御手段5へ送信され、該制御手段5によりパラメータ判断手段6が起動される。該パラメータ判断手段6では、サーバ1上の上記サービスディレクトリ2以外の他のディレクトリ3に設けられたデータベースに予め蓄積されたデータに基づいてユーザ端末10より送信されてきた上記ユーザIDが存在するか、また上記パスワードが正しいのかのチェック(S5)を行っている。

【0017】その結果、上記限定コンテンツBへのアクセス許可が与えられたユーザであると判断した場合、アクセス手段7が上記パラメータに対応して予め設定された限定コンテンツBの初期HTMLページ(例えば図4に示すメニューページ等)へアクセス(S6)を行い、該初期HTMLページを上記パスワードページと同様に上記ユーザ端末10へ送信し、上記表示装置13に表示(S7)させる。この初期HTMLページには少なくとも1つの次表示項目21(例えば図4に示すメニューページでは次に表示することのできるHTMLページの項目等)が掲げられており、ユーザが該次表示項目21のいずれかを指示することによって、次画面を選択することができるようになっている。すなわち、上記次表示項目21にはそれぞれに該次表示項目の格納場所のディレクトリを記載したフルパスの表示HTML名22がユーザには見えない形式(画面には表示されず上記ユーザ端末10のメモリ等に格納される)で隠しパラメータとして付与されており、また該フルパスの表示HTML名22に追加して上記アクセス手段7を起動する旨の指定がなされている。これによって、上記のようにユーザの指示に基づいて選択された特定の次表示項目21に対応した次画面を表示することができる。

【0018】尚、上記チェックの結果、上記限定コンテンツBへのアクセス許可が与えられたユーザでないと判

断した場合、上記初期HTMLページへのアクセスは行われず、アクセス許可がない旨の表示が上記表示装置13になされる(S8)。

【0019】次に、ユーザが選択した上記次表示項目21を実行(S9)すれば、該次表示項目21のフルパスの表示HTML名22がパラメータとして上記パスワードページのURLと同様にして上記制御手段5に送信され上記アクセス手段7が起動される。該アクセス手段7では送信されたパラメータであるフルパスの表示HTML名22によって選択された次表示をアクセス(S10)して、該次表示が上記パスワードページと同様にしてユーザ端末10へ送信され、上記表示装置13に表示(S11)される。これ以降の限定コンテンツBの次表示へのアクセスは、上記次表示へのアクセス手順と同様にして行われる。

【0020】また、上記限定コンテンツBを利用中のユーザは、どの時点であっても閲覧中の画面に設けられたリンクを上記入力手段14で選択して実行するか、または上記ブラウザ上から直接一般公開コンテンツAのURLを上記入力手段14で入力することによって、上記限定コンテンツBの閲覧を終了して一般公開コンテンツAの閲覧に移ることができる。

【0021】

【発明の効果】本発明のインターネットのコンテンツセキュリティ方法およびシステムによれば、限定コンテンツをサーバ上のサービスディレクトリ以外の他のディレ

クトリに設け、アクセス許可が与えられたユーザよりのアクセスであると判断した場合に上記限定コンテンツをアクセスするアクセス手段を上記サーバ上のサービスディレクトリに設けたことにより、該限定コンテンツへのアクセス許可が与えられていないユーザからのアクセスを確実に防止することができる。

【図面の簡単な説明】

【図1】本発明の適用されるネットワークの概念図である。

【図2】本発明の一実施例のブロック図である。

【図3】本発明の一実施例のフロー図である。

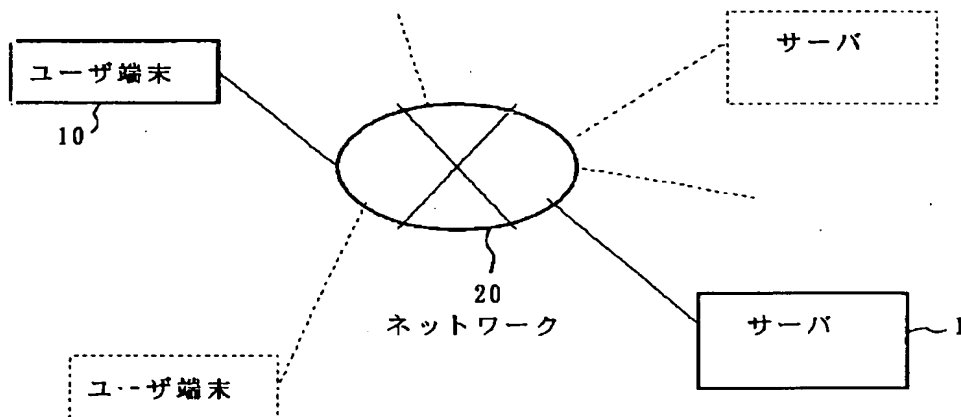
【図4】本発明の一実施例の画面例である。

【図5】従来のシステム概念図である。

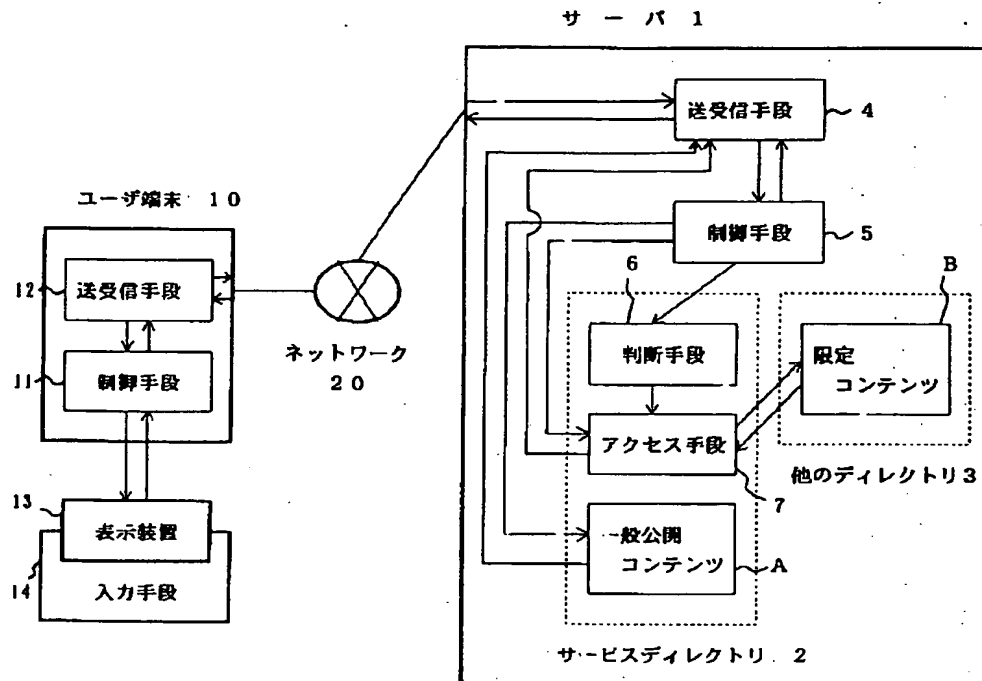
【符号の説明】

- |       |            |
|-------|------------|
| 1、31  | サーバ        |
| 2 32  | サービスディレクトリ |
| 3     | 他のディレクトリ   |
| 4、12  | 送受信手段      |
| 5、11  | 制御手段       |
| 6     | パラメータ判断手段  |
| 7     | アクセス手段     |
| 10、33 | ユーザ端末      |
| 13    | 表示装置       |
| 20、34 | ネットワーク     |
| A     | 一般公開コンテンツ  |
| B     | 限定コンテンツ    |

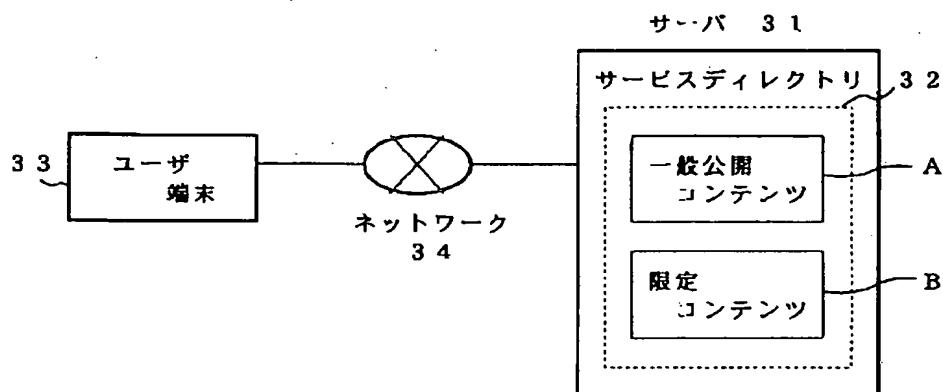
【図1】



【図2】



【図5】

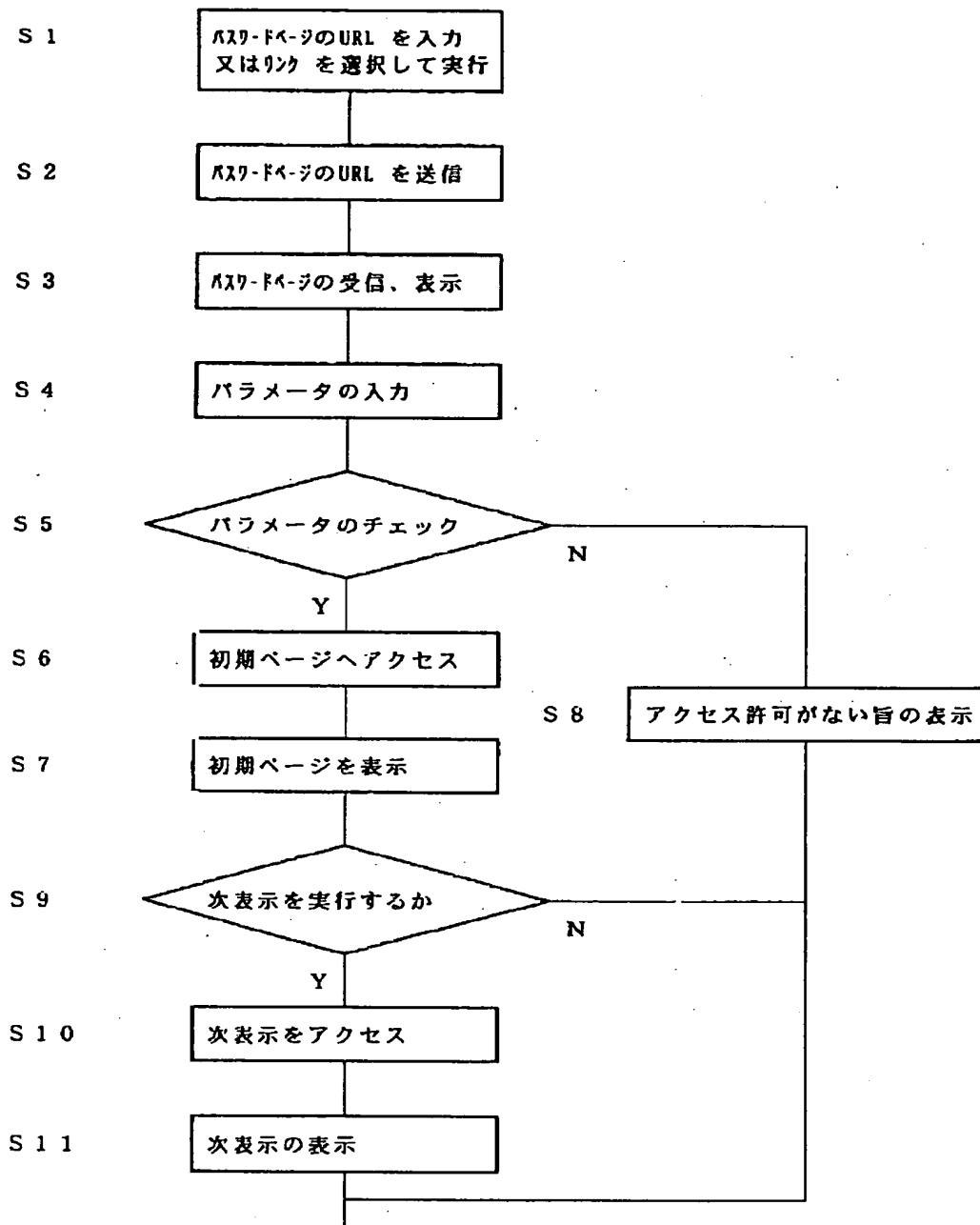


# BEST AVAILABLE COPY

(6)

特開平10-275114

【図3】



【図4】

